DIGITAL INFORMATION CIPHERING DEVICE AND DIGITAL INFORMATION REPRODUCTION DEVICE

Patent Number: JP2000252974
Publication date: 2000-09-14
Inventor(s): TAKAHASHI TETSUYA; MORITA KOJI; YAMASHITA TOSHIRO
Applicant(s):: KOBE STEEL LTD
Requested Patent: ☐ JP2000252974 (JP00252974)
Application Number: JP19990054927 19990303
Priority Number(s):
IPC Classification: H04L9/14 ; G11B20/10 ; H04L9/06 ; H04L9/18 ; H04N7/167
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To provide a digital information ciphering device and a digital information reproduction device by which an arithmetic amount required for decoding is reduced, deterioration in difficulty of encryption interpretation is minimized and information is reproduced in real time in spite of an inexpensive device configuration.
SOLUTION: A prescribed 1st area of a digital information stream being an object of encryption is encrypted together with an encryption key used for encrypting a 2nd area other than the 1st area. Thus, even when the 2nd area is encrypted by a simple encryption method, so long as the 1st area is encrypted with a method having high difficulty of interpretation, the difficulty of interpretation for the entire digital information stream is kept high. Furthermore, when the 1st area is set to a header part area of the digital information stream, even if a decoding arithmetic amount of this part is increased, only a slight delay is caused to start reproduction of information. Thus, deterioration in the difficulty of encryption interpretation can be minimized while reducing the arithmetic amount required for decoding and even a reproduction device with an inexpensive configuration can reproduce the information in real time.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－252974
（P2000－252974A）
(43)公開日　平成12年９月14日(2000.9.14)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	５Ｃ０６４
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｄ０４４
Ｈ０４Ｌ　9/06		Ｈ０４Ｌ　9/00	６１１Ｚ	５Ｊ１０４
9/18			６５１	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ	

審査請求　未請求　請求項の数９　ＯＬ　（全８頁）

(21)出願番号　特願平11－54927

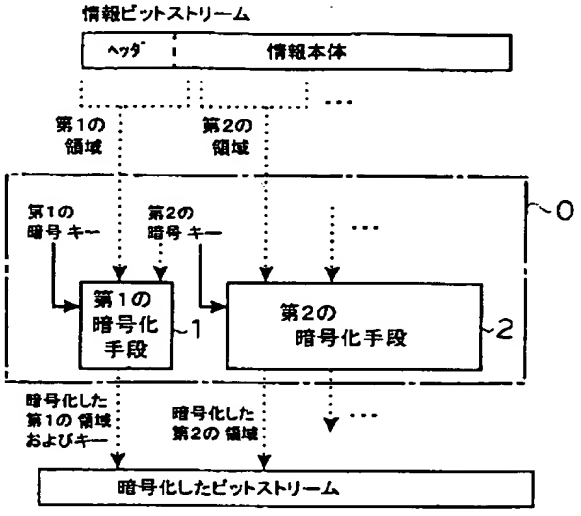
(22)出願日　平成11年３月３日(1999.3.3)

(71)出願人　000001199
株式会社神戸製鋼所
兵庫県神戸市中央区脇浜町１丁目３番18号
(72)発明者　高橋　哲也
兵庫県神戸市西区高塚台１丁目５番５号
株式会社神戸製鋼所神戸総合技術研究所内
(72)発明者　森田　孝司
兵庫県神戸市西区高塚台１丁目５番５号
株式会社神戸製鋼所神戸総合技術研究所内
(74)代理人　100084135
弁理士　本庄　武男

最終頁に続く

(54)【発明の名称】　ディジタル情報暗号化装置，及びディジタル情報再生装置

(57)【要約】
【課題】　復号化に要する演算量を低減させつつ，暗号解読の困難性の低下を最小限に抑えることができ，安価な装置構成でもリアルタイムの情報再生を可能とするディジタル情報暗号化装置，及びディジタル情報再生装置を提供する。
【解決手段】　暗号化対象であるディジタル情報における所定の第１の領域を，それ以外の第２の領域の暗号化に用いられる暗号化鍵と共に暗号化する。これにより，上記第２の領域を簡易な暗号化手法によって暗号化したとしても，上記第１の領域の暗号化を解読困難性の高い強固なものにしておけば，ディジタル情報全体としての解読困難性は高く維持される。更に，上記第１の領域を上記ディジタル情報の先頭部分の領域に設定すれば，この部分の復号化演算量が増加しても，情報の再生開始までに若干の遅れを生じるだけである。従って，復号化に要する演算量を低減させつつ，暗号解読の困難性の低下を最小限に抑えることができ，安価な構成の再生装置でもリアルタイムの情報再生が可能となる。



1

【特許請求の範囲】

【請求項１】　暗号化対象であるディジタル情報における所定の第１の領域を暗号化する第１の暗号化手段と，上記ディジタル情報における所定の第２の領域を暗号化する第２の暗号化手段とを具備すると共に，上記第１の暗号化手段が，上記第２の暗号化手段で用いる暗号化鍵を含めて上記第１の領域の暗号化を行うように構成されてなることを特徴とするディジタル情報暗号化装置。

【請求項２】　上記第１の暗号化手段が，上記第２の暗号化手段よりも解読困難性の高い暗号化方法を用いて暗号化する請求項１記載のディジタル情報暗号化装置。

【請求項３】　上記第１の暗号化手段が，上記第２の暗号化手段よりも単位データ量当たりの演算量をより多く要する暗号化方法を用いて暗号化する請求項２記載のディジタル情報暗号化装置。

【請求項４】　上記第１の領域が，上記ディジタル情報の先頭部分の領域である請求項２又は３記載のディジタル情報暗号化装置。

【請求項５】　上記第１及び第２の領域が，上記ディジタル情報の中の部分的な領域である請求項１～４のいずれかに記載のディジタル情報暗号化装置。

【請求項６】　上記第１及び第２の領域に，その他の領域の情報の再生に必要な情報が含まれてなる請求項５記載のディジタル情報暗号化装置。

【請求項７】　上記第１若しくは第２の領域に，上記ディジタル情報のヘッダ情報が含まれてなる請求項１～６のいずれかに記載のディジタル情報暗号化装置。

【請求項８】　上記ヘッダ情報に，著作権保護に用いられる情報が含まれてなる請求項７記載のディジタル情報暗号化装置。

【請求項９】　所定の第１の領域が所定の第２の領域の暗号化に用いられた暗号化鍵を含めて暗号化されているディジタル情報に対して，上記第１の領域を復号化し，上記第２の領域の暗号化鍵を取得する第１の復号化手段と，上記第１の復号化手段で得られた上記暗号化鍵を用いて，上記第２の領域を復号化する第２の復号化手段とを具備してなることを特徴とするディジタル情報再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，ディジタル情報を暗号化するディジタル情報暗号化装置，及び暗号化されたディジタル情報を再生するディジタル情報再生装置に関するものである。

【０００２】

【従来の技術】近年，音楽，映像などの情報はディジタル化された状態で流通されることが多くなってきた。そのため，著作権を保護する手段の一例として上記ディジタル情報に暗号化処理を施すことが行われている。ところが，暗号化されたディジタル情報の復号化には多くの

2

演算量が必要であるため，暗号化された情報をリアルタイムに再生するためにはそれなりのハードウェア資源が必要となる。しかしながら，例えば携帯型の情報再生装置などでは，コストやサイズなどの制約から，高性能のハードウェア資源を搭載するには限界がある。そこで，安価な装置構成でもリアルタイムの情報再生を可能とする暗号化方法が，例えば特開平１０－１４５７７３号公報に提案されている。上記暗号化方法は，ＭＰＥＧ２などでディジタル圧縮符号化された動画データに対して，フレーム内符号化画像（Ｉピクチャ）のみを暗号化するものである。上記フレーム内符号化画像以外のフレーム間予測符号化画像（Ｐピクチャ，Ｂピクチャ）は，上記フレーム内符号化画像を用いなくては復号化できないから，上記フレーム内符号化画像のみを暗号化することにより，解読の困難性を維持しながら復号化に要する総演算量を低減できるとしている。

【０００３】

【発明が解決しようとする課題】しかしながら，上記従来の暗号化方法では，単に暗号化対象領域を一部の領域に絞り込んでいるだけであるため，復号化に要する総演算量が低減される分だけ暗号解読の困難性も低減されてしまうという問題点があった。また，復号化に要する総演算量は低減できても，暗号化対象フレームのみに注目すればその復号化に要する演算量は変わらないため，リアルタイムの再生を行うためには結局従来と同じ高速な演算器を搭載するか，或いは上記暗号化対象フレームでの処理遅延を吸収できるだけの大きなバッファを搭載する必要があり，コスト低減や小型化というメリットは期待できない。本発明は上記事情に鑑みてなされたものであり，その目的とするところは，復号化に要する演算量を低減させつつ，暗号解読の困難性の低下を最小限に抑えることができ，安価な装置構成でもリアルタイムの情報再生を可能とするディジタル情報暗号化装置，及びディジタル情報再生装置を提供することである。

【０００４】

【課題を解決するための手段】上記目的を達成するために，第１の発明は，暗号化対象であるディジタル情報における所定の第１の領域を暗号化する第１の暗号化手段と，上記ディジタル情報における所定の第２の領域を暗号化する第２の暗号化手段とを具備すると共に，上記第１の暗号化手段が，上記第２の暗号化手段で用いる暗号化鍵を含めて上記第１の領域の暗号化を行うように構成されてなることを特徴とするディジタル情報暗号化装置として構成されている。ここで，上記第１の暗号化手段は，上記第２の暗号化手段よりも解読困難性の高い，例えば単位データ量当たりの演算量をより多く要する暗号化方法を用いて暗号化すれば，暗号化対象情報の大部分を占める第２の領域の復号化演算を少なくしたままで，情報全体としての解読困難性を高めることができる。更に，上記第１の領域を上記ディジタル情報の先頭部分の

領域に設定すれば，この部分の復号化演算量が増加しても，情報の再生開始までに若干の遅れを生じるだけであり，情報のリアルタイム再生に支障を来すことはない。また，上記第１及び第２の領域を，上記ディジタル情報の中の部分的な領域とすれば，復号化における演算量を更に低減させることができる。この時，上記第１及び第２の領域に，例えばその他の領域の情報の再生に必要な情報などのなるべく重要な情報が含まれるようにすれば，情報の違法再生の防止効果は高くなる。また，上記第１若しくは第２の領域に，著作権保護に用いられる情報が格納されたヘッダ情報が含まれるようにすれば，それら重要情報が直接暗号化されるため，望ましい。また，第２の発明は，上記第１の発明によって暗号化されたディジタル情報を再生する装置であって，所定の第１の領域が所定の第２の領域の暗号化に用いられた暗号化鍵を含めて暗号化されているディジタル情報に対して，上記第１の領域を復号化し，上記第２の領域の暗号化鍵を取得する第１の復号化手段と，上記第１の復号化手段で得られた上記暗号化鍵を用いて，上記第２の領域を復号化する第２の復号化手段とを具備してなることを特徴とするディジタル情報再生装置として構成されている。

【０００５】

【作用】本発明によれば，暗号化対象であるディジタル情報における所定の第１の領域が，それ以外の第２の領域の暗号化に用いられる暗号化鍵と共に暗号化される。従って，上記第２の領域を簡易な暗号化手法によって暗号化したとしても，上記第１の領域の暗号化を解読困難性の高い強固なものにしておけば，ディジタル情報全体としての解読困難性は高く維持される。更に，上記第１の領域を上記ディジタル情報の先頭部分の領域に設定すれば，この部分の復号化演算量が増加しても，情報の再生開始までに若干の遅れを生じるだけである。従って，復号化に要する演算量を低減させつつ，暗号解読の困難性の低下を最小限に抑えることができ，安価な構成の再生装置でもリアルタイムの情報再生が可能となる。

【０００６】

【発明の実施の形態】以下，添付図面を参照して本発明の実施の形態及び実施例につき説明し，本発明の理解に供する。尚，以下の実施の形態及び実施例は，本発明を具体化した一例であって，本発明の技術的範囲を限定する性格のものではない。ここに，図１は本発明の実施の形態に係る暗号化装置０の概略構成，及びその暗号化処理の概略を示すフローブロック図，図２は上記暗号化装置０に対応する再生装置１０の概略構成，及びその復号化処理の概略を示すフローブロック図，図３は本発明の実施例に係る暗号化装置０′の概略構成，及びその暗号化処理の概略を示すフローブロック図，図４は上記暗号化装置０′に対応する再生装置１０′の概略構成，及びその復号化処理の概略を示すフローブロック図である。本実施の形態に係る暗号化装置０は，図１に示すように，第１の暗号化手段１と第２の暗号化手段２とを具備して構成されている。上記第１の暗号化手段１は，暗号化対象である情報ビット列の先頭部分にあたる第１の領域を，上記第２の暗号化手段２で用いられる第２の暗号化鍵を含めて暗号化する。上記第１の領域は，例えば情報ビット列のヘッダ情報を含む領域である。上記第１の暗号化手段１で用いる暗号化方式としては，例えば公知のＤＥＳ(Data Encryption Standard)や公開鍵方式の暗号化など，解読の困難性の高い手法を用いることが望ましい。これらの解読困難性の高い暗号化アルゴリズムを用いると，一般に復号化に多くの演算量が必要とされるが，この暗号化が行われるのは情報の先頭部分のみであるため，その復号化に時間を要したとしても，情報の再生開始までに若干の遅れを生じるだけであり，情報のリアルタイム再生に支障を来すことはない。

【０００７】また，上記第２の暗号化手段２は，暗号化対象である情報ビット列のうち，上記第１の領域以外の領域（第２の領域とする）を暗号化する。この第２の暗号化手段２で用いる暗号化方式は，上記第１の暗号化手段１で用いたものに比べて簡易な手法を用いることが望ましい。例えば，鍵を用いて乱数など決まったルールで次々とビットパターンを発生させ，そのビットパターンと元の情報ビットとの排他的論理和をとる方法などが考えられる。或いは，乱数以外の更に簡易なルールによって鍵を加工して得られるビット列を排他的論理和のためのビットパターンとしてもよいし，鍵自体を固定のビットパターンとして用いてもよい。また，排他的論理和ではなく，元の情報ビット列を並べ替える方法などでもよい。これら以外にも種々の方法が考えられ，それぞれ解読の困難性に差が生じるが，再生装置に搭載可能なハードウェアとの兼ね合いなどによって適当な方法を用いればよい。暗号化対象である情報ビット列の大部分を占める上記第２の領域の暗号化に，復号化演算量の少ないこれらの簡易な暗号化手法を用いることにより，簡易なハードウェアを用いた再生装置によっても情報のリアルタイム再生が可能となる。勿論，上記のような簡易な暗号化では一般に暗号解読の困難性は低いが，その暗号化に用いられる鍵は上記第１の領域と共に強力な暗号化アルゴリズムによって暗号化されているため，復号化演算量の減少による暗号解読の困難性の低下は最小限に抑えられる。

【０００８】上述した暗号化装置０で暗号化された情報は，図２に示すような再生装置１０で再生される。上記再生装置１０は，第１の復号化手段１１と，第２の復号化手段１２とを具備して構成されている。上記第１の復号化手段１１は，復号化対象である情報ビット列の先頭の第１の領域を復号化する。この第１の領域の復号化には，上記暗号化装置０の第１の暗号化手段１で用いられた暗号化手法に対応して，例えばＤＥＳなどの復号化アルゴリズムが用いられる。このＤＥＳなどによる復号化

には多くの演算量が必要となるが，この復号化が行われるのは情報の先頭部分のみであるため，情報の再生開始までに若干の遅れを生じるだけであり，情報のリアルタイム再生に支障を来すことはない。上記第１の復号化手段１１による上記第１の領域の復号化に伴って上記第２の復号化手段１２で用いる第２の暗号化鍵が出力される。上記第２の復号化手段１２では，上記第２の暗号化鍵を用いて上記第１の領域以外の第２の領域の復号化が行われる。この第２の領域は比較的簡易な暗号化手法によって暗号化されているため，復号化演算量も少なくてすみ，上記第２の復号化手段１２を簡易なハードウェアによって構成したとしても情報のリアルタイム再生が可能である。

【０００９】以上説明したように，本実施の形態に係る暗号化装置０では，暗号化対象であるディジタル情報ビット列における先頭部分である第１の領域が，それ以外の第２の領域の暗号化に用いられる暗号化鍵を含めて解読困難性の高い暗号化手法によって暗号化されるため，上記第２の領域の暗号化に復号化時の演算量の少ない簡易な暗号化手法を用いて復号化演算量を減少させても，暗号解読の困難性の低下は最小限に抑えられる。また，上記第１の領域の暗号化に解読困難性の高い暗号化アルゴリズムを用いることによってその部分の復号化に多くの演算量が必要とされるが，この暗号化が行われるのは情報の先頭部分のみであるため，その復号化に時間を要したとしても，情報の再生開始までに若干の遅れを生じるだけであり，情報のリアルタイム再生に支障を来すことはない。

【００１０】

【実施例】上記実施の形態に係る暗号化装置０では，暗号化対象である情報ビット列の全領域に暗号化を施すこととしたが，情報ビット列の部分的な領域にのみ暗号化を施すようにすれば，復号化演算量を更に減少させることができる。一例を，図３を用いて説明する。本実施例に係る暗号化装置０′は，情報ビット選択分離手段３と，暗号化手段４と，暗号化ビット統合手段５とを具備して構成されている。上記情報ビット選択分離手段３は，暗号化対象である情報ビット列のうち，先頭部分の第１の領域以外の第２の領域から所定のビットのみを選択し，それら選択されたビットを上記暗号化手段４へ，それ以外のビットを上記暗号化ビット統合手段５へ送る。ここで，上記情報ビット選択分離手段３による暗号化対象ビットの選択方法としては，例えばＮバイト毎に分割された各ブロックにおけるある規則で決められた位置のｎビットを選択するようにしてもよいが，情報を再生する上で重要な情報を表すビット，例えばそれらの情報がなければ他のビットの再生を正しく行えないようなビットを選択することが有効である。例えば，音声やオーディオデータでは，スペクトル包絡，ゲイン，ピッチなどに対応する情報が特に重要であり，これらの情報を表すビットを暗号化対象ビットとすることが望ましい。スペクトル包絡パラメータとしては，ＬＳＰやＬＰＣ係数，反射係数などがよく知られており，それらの情報から音のスペクトル全体の外形が復元できる。また，ピッチには音の中に特に多く含まれる周波数成分に関する情報が含まれ，ゲインは音量に関する情報であるから，これらの情報があれば音のスペクトルに関するかなりの情報が復元できる。逆に言えば，これらの情報がなければ情報を正しく復元することは不可能である。携帯電話などで用いられるＣＥＬＰ系の音声圧縮やＴｗｉｎＶＱなどのオーディオ圧縮方式では，これらのパラメータが符号化データの中に含まれるが，全体のビットの中でのそれらの割合は僅かである。従って，これらの情報に関するビットを暗号化対象ビットとして選択すれば，演算量の削減と違法再生の防止の両面での効果が期待できる。暗号化手段４では，上記第１の領域と，上記情報ビット選択分離手段３で選択された暗号化対象ビットとが暗号化される。上記第１の領域としては，ヘッダに相当する最初のＮバイトとしてもよいし，そのＮバイトのうちのある規則で選ばれたいくつかのビットとしてもよい。上記ヘッダには，著作権者名，オリジナルかコピーかの区別，コピー可能回数などの著作権保護に関する重要な情報が含まれているため，これらの情報を暗号化しておくことは有効である。尚，上記暗号化手段４は，上記暗号化装置０における第１，第２の暗号化手段と同様の構成とし，第１の暗号化手段で上記第１の領域（第２の暗号化手段による暗号化鍵を含む）を，第２の暗号化手段で上記情報ビット選択分離手段３で選択された暗号化対象ビットをそれぞれ暗号化するように構成することが望ましい。上記暗号化ビット統合手段５では，上記暗号化手段４で暗号化された上記第２の領域の暗号化対象ビットと，上記情報ビット選択分離手段３から直接受け取った上記第２の領域の非暗号化ビットとが統合され，暗号化した第２の領域のビット列として出力する。出力された上記第２の領域のビット列は，上記暗号化手段４から出力された上記第１の領域の暗号化ビット列と統合されて暗号化ビット列として出力される。

【００１１】上述した暗号化装置０′で暗号化された情報は，図４に示すような再生装置１０′で再生される。上記再生装置１０′は，暗号化ビット選択分離手段１３と，復号化手段１４と，情報ビット統合手段１５とを具備して構成されている。上記暗号化ビット選択分離手段１３は，復号化対象である情報ビット列のうち，先頭部分の第１の領域以外の第２の領域から暗号化された所定のビットのみを選択し，それら選択されたビットを上記復号化手段１４へ，それ以外の非暗号化ビットを上記情報ビット統合手段１５へ送る。復号化手段１４では，復号化対象である情報ビット列の先頭部分の第１の領域と，上記暗号化ビット選択分離手段１３で選択された暗号化ビットとが復号化される。上記復号化手段１４によ

る上記第１の領域の復号化に伴って，上記暗号化ビット選択分離手段１３で選択された第２の領域内の暗号化ビットの暗号化鍵（第２の暗号化鍵）が出力される。上記復号化手段１４では，上記第２の暗号化鍵を用いて上記暗号化ビット選択分離手段１３で選択された暗号化ビットの復号化が行われる。この第２の領域は比較的簡易な暗号化手法によって，限られたビットのみが暗号化されているため，復号化演算量は上記実施の形態に係る再生装置１０と比べて更に少なくてすみ，上記復号化手段１４を更に簡易なハードウェアによって構成したとしても情報のリアルタイム再生が可能である。尚，上記実施の形態，及び実施例では，上記第１の領域を情報ビット列の先頭に設定したが，必ずしも先頭ビットを含まなければならないというものではない。情報のリアルタイム再生に支障がない範囲で任意の領域に設定できる。

【００１２】

【発明の効果】以上説明したように，第１の発明は，暗号化対象であるディジタル情報における所定の第１の領域を暗号化する第１の暗号化手段と，上記ディジタル情報における所定の第２の領域を暗号化する第２の暗号化手段とを具備すると共に，上記第１の暗号化手段が，上記第２の暗号化手段で用いる暗号化鍵を含めて上記第１の領域の暗号化を行うように構成されてなることを特徴とするディジタル情報暗号化装置として構成されているため，上記第２の領域を簡易な暗号化手法によって暗号化したとしても，ディジタル情報全体としての解読困難性の低下を抑えることができる。このように，復号化に要する演算量を低減させつつ，暗号解読の困難性の低下を抑えることができるため，安価な構成の再生装置でもリアルタイムの情報再生が可能となる。ここで，上記第１の暗号化手段は，上記第２の暗号化手段よりも解読困難性の高い，例えば単位データ量当たりの演算量をより多く要する暗号化方法を用いて暗号化すれば，暗号化対象情報の大部分を占める第２の領域の復号化演算を少なくしたままで，情報全体としての解読困難性の低下を更に抑えることができる。更に，上記第１の領域を上記ディジタル情報の先頭部分の領域に設定すれば，この部分の復号化演算量が増加しても，情報の再生開始までに若干の遅れを生じるだけであり，情報のリアルタイム再生に支障を来すことはない。また，上記第１及び第２の領域を，上記ディジタル情報の中の部分的な領域とすれば，復号化における演算量を更に低減させることができる。この時，上記第１及び第２の領域に，例えばその他の領域の情報の再生に必要な情報などのなるべく重要な情報が含まれるようにすれば，情報の違法再生の防止効果は高くなる。また，上記第１若しくは第２の領域に，著作権保護に関する情報が格納されたヘッダ情報が含まれるようにすれば，それら重要情報が直接暗号化されるため，望ましい。また，第２の発明は，上記第１の発明によって暗号化されたディジタル情報を再生する装置であって，所定の第１の領域が所定の第２の領域の暗号化に用いられた暗号化鍵を含めて暗号化されているディジタル情報に対して，上記第１の領域を復号化し，上記第２の領域の暗号化鍵を取得する第１の復号化手段と，上記第１の復号化手段で得られた上記暗号化鍵を用いて，上記第２の領域を復号化する第２の復号化手段とを具備してなることを特徴とするディジタル情報再生装置として構成されているため，安価な構成でリアルタイムの情報再生が可能である上に，違法再生の防止効果も高く維持される。

【図面の簡単な説明】

【図１】　本発明の実施の形態に係る暗号化装置０の概略構成，及びその暗号化処理の概略を示すフローブロック図。

【図２】　上記暗号化装置０に対応する再生装置１０の概略構成，及びその復号化処理の概略を示すフローブロック図。

【図３】　本発明の実施例に係る暗号化装置０′の概略構成，及びその暗号化処理の概略を示すフローブロック図。

【図４】　上記暗号化装置０′に対応する再生装置１０′の概略構成，及びその復号化処理の概略を示すフローブロック図。

【符号の説明】

０，０′…暗号化装置（ディジタル情報暗号化装置の一例）

１…第１の暗号化手段

２…第２の暗号化手段

３…情報ビット選択分離手段

４…暗号化手段

５…暗号化ビット統合手段

１０，１０′…再生装置（ディジタル情報再生装置の一例）

１１…第１の復号化手段

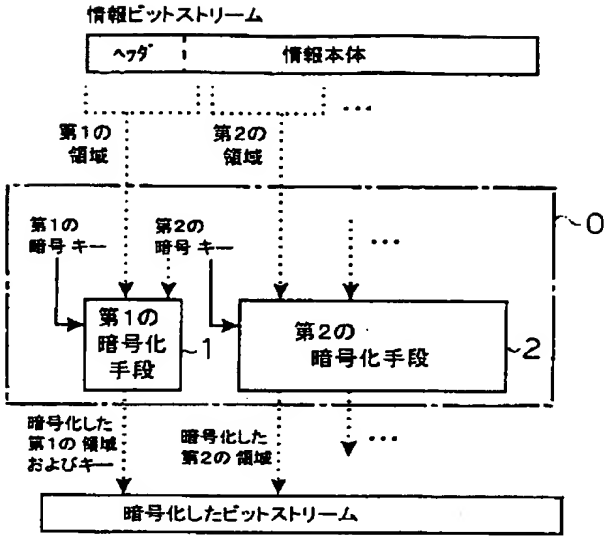
１２…第２の復号化手段

１３…暗号化ビット選択分離手段

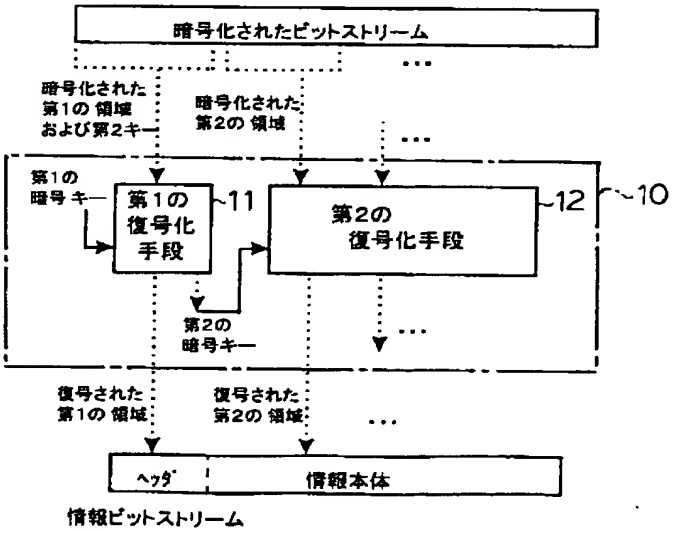
１４…復号化手段

１５…情報ビット統合手段

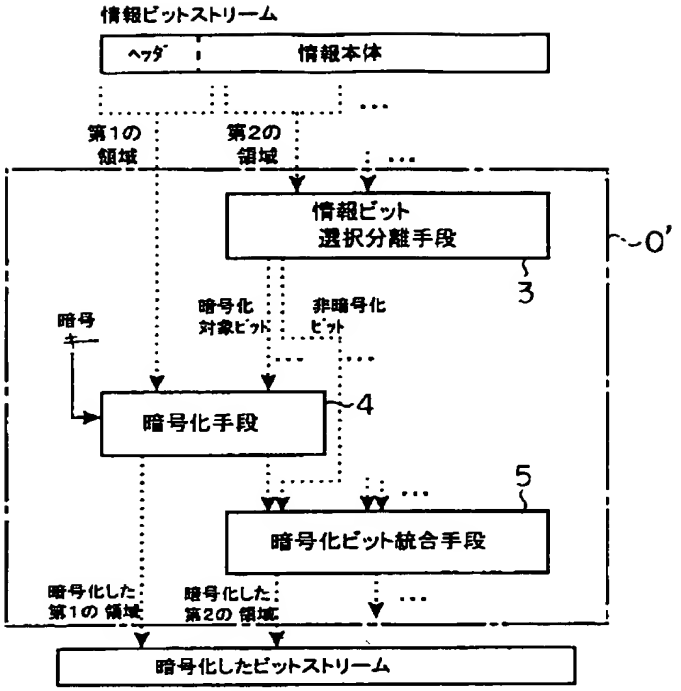
【図１】


情報ビットストリーム
ﾍｯﾀﾞ
情報本体
第1の領域
第2の領域
第1の暗号キー
第2の暗号キー
第1の暗号化手段
1
第2の暗号化手段
2
0
暗号化した第1の領域およびキー
暗号化した第2の領域
暗号化したビットストリーム

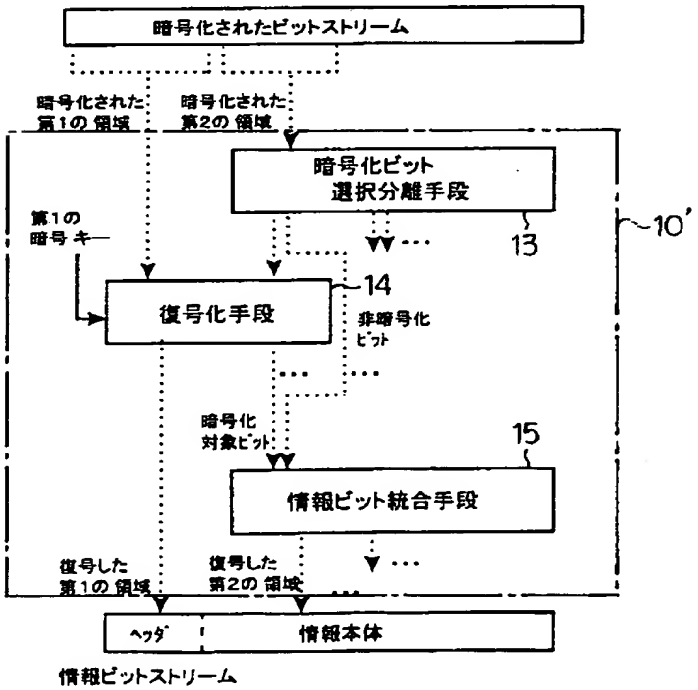
【図２】


暗号化されたビットストリーム
暗号化された第1の領域および第2キー
暗号化された第2の領域
第1の暗号キー
第1の復号化手段
11
第2の復号化手段
12
10
第2の暗号キー
復号された第1の領域
復号された第2の領域
ﾍｯﾀﾞ
情報本体
情報ビットストリーム

【図３】


情報ビットストリーム
ヘッダ
情報本体
第1の領域
第2の領域
情報ビット選択分離手段
3
10'
暗号キー
暗号化対象ビット
非暗号化ビット
暗号化手段
4
5
暗号化ビット統合手段
暗号化した第1の領域
暗号化した第2の領域
暗号化したビットストリーム

【図４】


暗号化されたビットストリーム
暗号化された第1の領域
暗号化された第2の領域
暗号化ビット選択分離手段
13
10'
第1の暗号キー
14
復号化手段
非暗号化ビット
暗号化対象ビット
15
情報ビット統合手段
復号した第1の領域
復号した第2の領域
ヘッダ
情報本体
情報ビットストリーム

フロントページの続き

(72)発明者　山下　俊郎
兵庫県神戸市西区高塚台１丁目５番５号
株式会社神戸製鋼所神戸総合技術研究所内

Ｆターム(参考)　5C064 CA14 CB01 CC04
5D044 DE03 GK17
5J104 AA01 AA16 AA18 EA17 JA03
NA03 PA14